AMENDMENTS TO THE CLAIMS

No claims are canceled.

No claims are added.

Claims 1, 12, and 25 are amended.

Claims 1-29 are pending.

1. (Currently amended) A method comprising:

establishing an authenticated session between a server and a client;

subsequent to establishing the authenticated session, receiving at the server, a request from the client;

subsequent to receiving at the server, a request from the client, determining whether the session is still authenticated;

in an event that the session is no longer authenticated, persisting as a pending request at the server, the request from the client; and

in an event that the session is subsequently re-authenticated, the server processing the pending request.

2. (Original) The method of claim 1 wherein the determining comprises verifying an authentication token associated with the client.

3. (Original) The method of claim 2 wherein the verifying comprises verifying that the authentication token has not timed out.

4. (Original) The method of claim 2 wherein the authentication token is a cookie stored by the client.

5. (Original) The method of claim 2 wherein the authentication token is part of the request received from the client.

6. (Original) The method of claim 2 wherein the authentication token is encrypted.

7. (Original) The method of claim 1 wherein persisting the request comprises storing the request in a file.

8. (Original) The method of claim 1 wherein persisting the request comprises storing the request in a database.

9. (Original) The method of claim 1 further comprising, after persisting the request, directing the client to authenticate the session.

10. (Original) The method of claim 9 wherein directing the client to authenticate the session comprises:

directing the client to a login module; and

directing the client to an address associated with the pending request.

11. (Original) The method of claim 10 wherein the address associated with the pending request is a URL.

12. (Currently amended) A method comprising:

establishing an authenticated session between a server and a client;

the client submitting a request to the server via the session;

subsequent to submitting the request, the client receiving an indication that the session is no longer authenticated;

the client obtaining a session re-authentication; and

the client receiving an indication that the request has been processed, without resubmitting the request.

13. (Previously presented) A server system comprising:

an authentication verifier configured to determine whether an initially authorized session between the server and a client is still authorized;

a client interface configured to receive a request from the client;

a pending request store configured to maintain the request in an event that the session is not authorized; and

a processing unit configured to process the request that is maintained in an event that the session is re-authorized.

14. (Previously presented) The system of claim 13 further comprising an authentication redirect generator configured to generate an instruction to redirect the client to obtain re-authorization for the session.

15. (Original) The system of claim 14 wherein the instruction is a URL.

16. (Original) The system of claim 14 wherein the authorization is an authentication token.

17. (Previously presented) An application server comprising the server system as recited in claim 13.

18. (Original) A system comprising:

a client interface configured to receive a request from a client;

an authentication token verifier configured to determine whether an authentication token associated with the client is valid;

a pending request store configured to store the request in an event that the authentication token associated with the client is not valid; and

an authentication redirect generator configured to generate an instruction to redirect the client to obtain a valid authentication token.

19. (Original) The system of claim 18 wherein the authentication token verifier is further configured to determine whether the authentication token has expired.

20. (Original) The system of claim 18 wherein the authentication redirect generator is further configured to direct the client to access the request that is stored.

21. (Original) The system of claim 18 wherein the pending request store is a database.

22. (Original) A system comprising:

means for receiving a request from a client;

means for determining whether an authentication token associated with the client is valid;

means for storing the request in an event that the authentication token is not valid; and

means for generating an instruction to redirect the client to obtain a valid authentication token.

23. (Previously presented) A system comprising:

a client;

an application server configured to:

establish an authenticated session with the client;

receive a request from the client;

maintain the request as a pending request in an event that the session is no longer authenticated; and

direct the client to re-authenticate the session;

the client being configured to re-authenticate the session by obtaining authentication from an authentication entity in response to direction from the application server, and the client further configured to subsequently access the pending request; and

upon client access to the pending request, the application server being further configured to process the pending request.

24. (Original) The system of claim 23 wherein the application server and the authentication entity are implemented as one server.

25. (Currently amended) One or more computer-readable media comprising computer executable instructions that, when executed, direct a computing system to:

establish a session with an authenticated client;

subsequent to establishing the session, receive a request from the client;

subsequent to receiving the request, determine whether the client is still authenticated;

in an event that the client is no longer authenticated, persist the request; and

in an event that the client is subsequently re-authenticated, process the request that is persisted.

26. (Previously presented) The one or more computer-readable media of claim 25 further comprising computer executable instructions that, when executed, direct a computing system to:

in the event that the client is no longer authenticated,

redirect the client to re-obtain authentication; and

direct the client to the request that is persisted.

27. (Previously presented) One or more computer-readable media comprising computer executable instructions that, when executed, direct a computing system to:

establish an authenticated session with a client;

receive a request from the client;

determine whether an authentication token associated with the client is still valid;

store the request if the authentication token is no longer valid; and

generate an instruction to redirect the client.

28. (Original) The one or more computer-readable media of claim 27 wherein the instruction comprises an instruction to redirect the client to obtain a valid authentication token.

29. (Original) The one or more computer-readable media of claim 28 wherein the instruction further comprises an instruction to redirect the client to the request that is stored upon the client obtaining the valid authentication token.